RE-EXAM
2700
1e

PATENT TC
6215-0000124/US/RED 2100,
Cpk2
2911

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Reissue App. No.: 09/694,416
Patent No. 5,848,159
Issued: 12/8/1998

Related to:
Re-Examination Control No. 90/005,733 and
Re-Examination Control No. 90/005,776

Filing Date: October 20, 2000

Applicant: Thomas Collins et al.

Examiner: James Seal Group Art Unit: 2131

Title: PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD

BOX REISSUE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

October 21, 2003

RESUBMISSION OF AMENDMENT IN REISSUE APPLICATION

Sir:

Further to a telephone conversation of October 17, 2003 with Examiner Laufer and applicants previous filing of October 14, 2003, applicants are submitting herewith amendments to the claims to comply with the Reissue rules. This resubmission is in triplicate (a copy for the related Re-Examination files) as required.

IN THE CLAIMS

4. (Three Times Amended) A [cryptographic] system for communications [system] of a message cryptographically processed with an RSA public key encryption comprising:

a communication [medium] channel for transmitting a ciphertext word signal C;

[an] encoding means coupled to said channel and adapted for transforming a transmit message word signal M to [a] the ciphertext word signal C [and for transmitting C on said channel, where M corresponds to a number representative of a message and $0 \leq M \leq n-1$ where n is a composite number] using a composite number, n, where n is a product of the form

$$n=p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

[where] k is an integer greater than 2, and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, [and] where [C] the transmit message word signal M corresponds to a number representative of [an enciphered form of said] the message and [corresponds to] $0 \leq M \leq n-1$

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

[$C \equiv M^e \pmod n$] $C \equiv M^e \pmod n$, and

where e is a number relatively prime to $\text{lcm}(p_1-1, p_2-1, \ldots, p_k-1)$; and

[a] decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and, having available to it the k distinct random prime number $p_1, p_2, \ldots p_k$, for transforming the ciphertext word signal C to a receive message word signal M' where M' corresponds to a number representative of a [deciphered] decoded form of the ciphertext word signal C [and corresponds to] through a relationship of the form

[$M' \equiv C^d \pmod n$] $M' \equiv C^d \pmod n$

where d is selected from the group consisting of [the] a class of numbers equivalent to a multiplicative inverse of

$$e(\text{mod}(\text{lcm}((p_1-1), (p_2-1), \ldots, (p_k-1)))).$$

7. Cancelled

13. Cancelled

New Claims:

35. (Twice Amended) The method according to claim [[14]] 9, wherein [[a]] the signed message word signal M_{1s}, formed from the digital message word signal M_1 being cryptographically processed [in accordance with the method is compatible with two-prime] at the fist terminal with multi-prime (k>2) RSA public key [cryptography] encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, ... [[pk]] p_k, is decipherable at the second terminal with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q.

REMARKS

This amendment is filed in response to the final office action mailed April 11, 2003.

I. STATUS OF THE CLAIMS

As of the date of this Amendment, claims 1-6 and 9-12, 14-61 remain pending. Claims 4 and 35 have been amended and claims 7 and 13 have been cancelled as a result of this response.

II. OBJECTION TO THE SPECIFICATION

A. New Matter

Sections 11-16 of the Office Action indicate that Applicants' previous amendment of September 16, 2002 has been objected to under 35 U.S.C. § 132 as having allegedly introduced new matter into the specification.

In Section 12, the Examiner objects to the replacement to the term "using" with the term "extending". Applicants assert that the conventional RSA scheme uses two primes, whereas the present invention uses three or more. In this context, Applicants believe that the present invention "extends" the number of primes from two to three or more. As a result, Applicants believe that the present invention "extends" the RSA scheme. Accordingly, reconsideration and withdrawal of the objection is respectfully requested.

In Section 13, the Examiner asserts that the change that "three or more random large, distinct primed numbers are developed and checked to ensure that each (p_i-1) is relatively prime to e" is new matter.

Applicants direct the Examiner's attention to originally filed independent claim 1, filed on January 16, 1997 which recites e is a number relatively prime to $(p_1-1) \cdot (p_2-1) \cdot \ldots (p_k-1)$.

Accordingly, Applicants respectfully submit that the change to column 5, lines 31-33, merely brings the specification into compliance with original claim 1. Further, Applicants respectfully submit that one of ordinary skill in the art would recognize that the equation recited at column 5, line 39 would not work if three or more random large distinct prime numbers were not relatively prime to e. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In Section 14, the Examiner asserts that the amendment to column 5, line 52, to add a digital signature, is not supported. However, Applicants have been unable to locate the addition of a "digital signature" in Applicants previous response. Clarification of this rejection is requested.

In Section 15, the Examiner asserts that the amendment to the specification to column 6, line 24 to change "$i \geq 2$" to "$2 \leq i \leq k$ where k is the number of primes in n" constitutes new matter.

Applicants respectfully submit that this change merely more accurately recites the teachings of the present invention. As set forth clearly throughout the specification, there are no prime numbers beyond p_k; accordingly, it makes absolutely no sense to indicate prime numbers greater than equal to 2, but unbounded by the number of prime numbers k. Accordingly, Applicants respectfully submit that this is not new matter, but merely a reflection of the upper bound of the number of k primes, which the change of which, Applicants believe more accurately represents the present invention. However, although less accurate, Applicants are willing to leave this portion of the specification as "$i \geq 2$".

In Section 16, with regard to column 6, line 65, the Examiner asserts that the change from "the decrypted message M can be obtained" to "the ciphertext C can be obtained" is new matter.

The Examiner further asserts that in the first version, summation is required, wherein the second version iteration is required.

In response to this objection, Applicants respectfully submit that there are at least two know solutions for the Chinese Remainder Theorem. The first, proposed by Gauss, is a summation technique, and therefore not recursive. The second, proposed by Garner, is a recursive technique. Applicants respectfully submit that the original patent describes Garner's technique beginning at column 6, line 1 and Gauss' technique, beginning at column 7, line 1. Since the present application supports both recursive and non-recursive solutions, Applicants assert that the Amendment to column 6, line 65 does not constitute new matter.

III. CLAIM OBJECTIONS

In Sections 21 and 22, the Examiner points out minor informalities in the previous amendments to claims 4 and 35. Applicants have amended claims 4 and 35 to correct these minor informalities.

IV. CLAIM REJECTIONS UNDER 35 U.S.C. § 112

A. 35 U.S.C. § 112, FIRST PARAGRAPH

In Section 24, claim 1 is rejected under 35 U.S.C. § 112, first paragraph but no specific rejection is set forth. Applicants assume this rejection is related to the objection to the specification under 35 U.S.C. § 132 and therefore traversed for the reasons set forth above.

In Sections 25 and 26, the Examiner asserts that claims 1-2, 18-19, 32-33, 37, 42-49, and 56-61 are rejected under 35 U.S.C. § 112, first paragraph, because the patent as originally filed does not disclose $k \geq 3$. Applicants respectfully submit that column 3, line 27-29 of the original

Collins et al. patent recite that it is an object of the present invention is to provide a system and method for utilizing "multiple (more than two) distinct prime number components to create n." Further, column 3, lines 40-41 of the original Collins et al. patent recite that "n is developed from three or more distinct prime numbers; i.e., $n = p_1 \cdot p_2 \cdot \ldots p_k$, where k is an integer greater than two." Finally, column 5, lines 66-67 recite an example assuming three distinct primes, p_1, p_2, and p_3. Accordingly, Applicants respectfully submit that an amendment reciting k is an integer greater than two is supported by multiple passages in the original Collins et al. patent.

In Sections 27-29, the Examiner asserts that claims 1-61 are rejected under 35 U.S.C. § 112, first paragraph, objecting to the term "random". The Examiner correctly points out that the term random is utilized in the original patent at column 5, line 31 and is therefore supported by the original patent. Applicants assert that this disclosure supports the claims as amended.

In Applicants previous Response, Applicants asserted that "the randomness and distinctness attributes of the k prime numbers will materially improve the security in any cryptographic system with RSA public key encryption".

With respect to this statement, the Examiner asserts that if this were the intent of the original patent, the original patent does not support this view. Applicants respectfully submit that the above statement is an advantage of the present invention. Advantages of the present invention need not be provided in the specification In re Chu, 36 U.S.P.Q.2d 1089 (Fed.Cir. 1995). Accordingly, Applicants respectfully submit that claims 1-61 are supported by the original specification, because random is provided in the original patent, and any purported advantage of the randomness need not be present in the original patent.

In Sections 30 and 31, the Examiner rejects claims 7 and 13 for failing to describe how the equation recited therein is carried out. Applicants direct the Examiner's attention to the cancellation of independent claims 7 and 13, which render this rejection moot.

B. 35 U.S.C. 112, SECOND PARAGRAPH

In Sections 32 and 33, the Examiner objects to the relationship in claims 7 and 13 as being used to mean an "RSA public encryption". Applicants direct the Examiner's attention to the cancellation of independent claims 7 and 13, which render this rejection moot.

In Section 34, the Examiner objects to amended claim 9, specifically the word "means" is not followed by a function. Applicants have reviewed claim 9 and are unsure of the Examiner's rejection, in particular, each means clause of claim 9 appears to recite a function.

VI. CLAIM REJECTION UNDER 35 U.S.C. § 103

A. SUMMARY OF CLAIM REJECTIONS

In sections 35-76 of the Office Action, claims 1-7, 9-61 are rejected under 35 U.S.C. § 103(a). In sections 36-65 of the Office Action, claims 1-7, 9-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 4,405,829 to Rivest et al., henceforth RSA, and further in view of Rivest et al. "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Communications of the ACM, 21(2) February 1978, henceforth Rivest and further in view of Knuth, The Art of Computer Programming Vol. 2, page 179.

In formulating the rejection of claims 1-7 and 9-61 in view of RSA, Rivest, and Knuth in paragraphs 35-39, the Examiner picks and chooses various portions of three publications to piece together the subject matter of the present claims. Applicants assert that it impermissible to use

the claimed invention as an instruction manual or template to piece together the teachings of the prior art so that the claimed invention is rendered obvious. It is established U.S. patent law that one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention.

Obviousness can not be established by combining the teachings of the prior art to produce the claimed invention, absent a teaching or suggestions supporting the combination. Under § 103, the teachings of references can be combined only if there is some suggestion or incentive to do so. Applicants further respectfully submit that this tenant of U.S. patent law also applies to separate embodiments of the same patent or patent publication. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of the RSA patent, the Rivest publication, and Knuth, in order to piece together the invention recited in the presently pending claims. Accordingly, Applicants respectfully submit that claims 1-7 and 9-61 are allowable for at least this reason.

In Sections 66-68, claims 7 and 13 are rejected in view of RSA and Rivest and further in view of Schwenk US 5,835,598. This rejection is moot in light of the cancellation of these claims.

In Sections 69-70, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 are rejected under 35 U.S.C. § 102(b) as being anticipated by Vanstone and Zuccherato, "Using four-prime RSA in which some bits are Specified", Electronic Letters, 30(25), 16 August 1994, henceforth Vanstone.

In paragraph 70, the Examiner asserts that "Vanstone selects random primes even though he makes bit assignments in an expanding product ...". Applicants respectfully submit that this statement is wholly unsupported by Vanstone. Vanstone makes absolutely no mention of

random prime numbers. Accordingly, Applicants respectfully submit that claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, and 60-61 are allowable for at least this reason.

In Sections 72-74, claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo (RSA Moduli Should Have 3 Prime Factors), and further in view of Rivest et al.

With respect to Nemo, Applicants respectfully assert that this publication was submitted by Applicants during prosecution of the original application with no date, since applicants were unable to ascertain the publication date of the Nemo paper. Nemo was printed on the front of U.S. Patent 5,848,159 with "No Date or Publication Given".

During the prosecution of the present application, the Examiner has adopted the publication date of Nemo as August 1996, relying on a footnote on page 1 which states "the original version of this article may be obtained from Scientific Bulgarian Magazine, August 1996". Applicants respectfully assert that the fact this paper was submitted by a pseudonym as "Captain Nemo" and alleges to have been published in a fictitious publication, namely "Scientific Bulgarian", casts sufficient doubt as the date of the publication to render it insufficient to be relied upon as prior art against the present application. As set forth in M.P.E.P. § 706.02(a), the Examiner must determine the issue or publication date of a reference of a proper comparison between the application and the reference dates can be made. Applicants respectfully assert that the fictitious author in a fictitious journal, namely "Scientific Bulgarian", cast doubt on the accuracy of August 1996 as a publication date. Until the Examiner is able to verify the publication date of the Nemo publication as qualifying as prior art against the present application under 35 U.S.C. § 102(a) or (b) Applicants respectfully submit that Nemo cannot be applied

against the present application. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In Section 75, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Itakura and Nakamura, A Public-Key Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No. 71, October, and further in view of Rivest et al. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

Initially, Applicants respectfully submit that the scheme described in Itakura and Nakamura provides no security. Accordingly, the purpose of this publication is completely different from the purpose of the present invention.

The goal of the Itakura et al. scheme is to create signatures appropriate for use in a business hierarchy. An individual at a higher level has a different "r" from an individual at a lower level and the lower level employee should not be able to forge the higher rank signature. Accordingly, Applicants respectfully submit that Itakura et al. is irrelevant to the present invention. Additionally, in exemplary embodiments of the present invention, all the primes are part of the private key and the security relies on the primes not being known. As set forth above, in Itakura et al., the third prime "r" is public. Accordingly, Applicants respectfully submit that claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are allowable over Itakura et al. for at least this reason. Additionally, an advantage of exemplary embodiments of the present invention is to obtain the security of a large "n" by increasing the number factors, instead of the size of the factors. In contrast, Itakura et al. stated in the first paragraph of 3.3 that increasing the length of the third prime "r" increases the length of "n" without increasing the security of the system.

For the reasons set forth above, Applicants respectfully assert that claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are allowable over Itakura et al. in view of Rivest et al.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 1-6, 8-12, and 14-61 in connection with the present application is earnestly solicited.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicant(s) hereby petition(s) for a three (3) month extension of time for filing a reply to the outstanding Office Action. The fee for extension fee of $950.00 is being paid under the Notice of Appeal concurrently filed herewith.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John A. Castellano at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-2025 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/cah

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the Amendment filed concurrently herewith, was served via first class mail, this 21st day of October, 2003 to:

Ronald L. Chichester
Frohwitter
Three Riverway, Suite 500
Huston, Texas 77056
Phone 713-621-0703
Fax 713-622-1624

John A. Castellano, Esq.

Copy of pp. No. 26

MAIL STOP AF
RESPONSE UNDER
37 C.F.R. § 1.116
EXPEDITED PROCEDURE
EXAMINING GROUP 2131

PATENT
/US

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	Thomas Collins et al.	Conf.:	
Appl. No.:	09/964,416	Group:	2131
Filed:	October 20, 2000	Examiner:	James Seal
For:	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD		

NOTICE OF APPEAL FROM THE PRIMARY EXAMINER TO THE BOARD OF APPEALS

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

October 14, 2003

Sir:

Applicants hereby appeal to the Board of Appeals from the decision dated April 11, 2003 of the Primary Examiner finally rejecting claims 1-7 and 9-61.

☐ The enclosed document is being transmitted via the Certificate of Mailing provisions of 37 C.F.R. § 1.8.

Applicants hereby petition for an extension of three (3) months pursuant to 37 C.F.R. §§ 1.17 and 1.136(a).

The fee has been calculated as shown below:

☒ NO extensions of time have been previously obtained for responding to the Final Rejection. Thus a fee of $950.00 is required for the full period of the above-requested extension of time.

☐ An extension of month(s) for responding to the Final Rejection is being paid with the filing of an Amendment attached hereto.

☐ Applicant claims small entity status. See 37 C.F.R. § 1.27.

The Government fee for filing a Notice of Appeal to the Board of Appeals is calculated as follows:

☒ Large entity - $330.00

☐ Small Entity - $165.00

Therefore, the TOTAL FEE due for the filing of this Notice of Appeal is $1,280.00

Payment of the above TOTAL FEE is being made in the following manner:

☐ Check in the amount of $.00 is enclosed.

☒ Please charge Deposit Account No. 08-2025 in the amount of $1,280.00. A triplicate copy of this sheet is attached.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-2025 for any additional fees required under 37 C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/cah